Remarks

Claim 1 has been amended by adding thereto the limitations previously found in claim 3 and claim 5. Claim 19 has been amended to include the limitation of dependent claim 20. It is respectfully submitted that these amendments place the application in condition for allowance as will be more fully explained or places the application in better form for appeal.

A banknote validator according to the present invention has a series of sensors for scanning of a banknote as it moves past the sensors. A central processing unit controls the operation of the validator and receives and processes the signals from the sensors. The validator includes a removable memory storage arrangement which is insertable in a receiving location of the validator. This removable memory storage arrangement when received in the receiving location, forms an electrical communication path with the central processing unit.

The central processing unit has a testing procedure which evaluates the integrity of any received removable memory storage arrangement. The central processing unit only downloads information from the storage arrangement upon a positive evaluation of the integrity of the removable memory storage arrangement. The claim as now amended further clarifies this testing procedure. The removable memory storage arrangement includes an electronic address which is received by the central processing unit. The removable flash memory module contains encrypted algorithms used by the central processing unit to evaluate banknotes and the central processing unit includes decryption software for decoding the algorithms and storing the coded algorithms in the central processing unit. This electronic address is used by the central processing unit to determine the authenticity of the removable memory storage arrangement.

With the above arrangement, a standalone banknote validator installed in a vending machine or other device can easily be updated by merely inserting the removable flash memory module into the appropriate port of the validator. The validator decrypts the material and evaluates the integrity of the removable flash memory module to determine whether it is authentic. If the evaluation is positive, the software of the validator is updated. With this arrangement, there is no requirement for the removable flash memory module to know the serial number or address information of the validator. The validator conducts its own evaluation of the integrity of the removable flash memory module based on information provided to it by the removable flash memory module.

In the preferred embodiment of the invention, as described on page 5 of the present application, the CPU obtains the identification code of the flash memory module from its read only memory. The CPU decodes the information provided to it and part of the decoded information contains the identification code of the removable flash memory module. If there is an agreement between these two numbers, it is assumed by the CPU that the software is authentic and has not been exposed to corruption.

From the above, it can be appreciated that the evaluation carried out by the validator is based on information provided to it by the removable flash memory module. The validator receives the information from the module and based on the information provided, conducts a test of the module's integrity. Neither the primary reference nor the secondary references operate in this manner.

It is acknowledged in the Official Action that the primary reference of Mazur et al., does not include any separate

evaluation of the integrity of the flash card that is used in the validator. Furthermore, there is no teaching that the removable memory module should have the software thereof encrypted to maintain the integrity of the system, nor does the CPU of the Mazur et al. reference have any capability of decrypting information.

The secondary reference of Meyer et al., is directed to an intelligent public telephone system and method. This patent is classified in international class H04M17/00 or U.S. class 379, subclass 145.

The primary reference of Mazur is in international class G07D7/12 or U.S. class 194, subclass 207; class 382, subclass 135.

It is noted that none of the international or U.S. classes overlap between these references and there is no overlap between the fields of search with respect to each of these references.

It is submitted that these are not analogous art as confirmed by the completely different international and U.S. classes and is further confirmed by the various classes that were searched.

It is further noted that intelligent public telephone systems and methods of the secondary reference of Meyer et al. is indeed remote and distinct from banknote validators associated with the testing of banknotes for either acceptance or rejection of the banknote in a currency transaction. It is submitted that it is only based on hindsight and with full knowledge of the present application that one would ever consider the secondary reference of Meyer et al. It is therefore argued that a person

skilled in the art would not make this combination and there is no suggestion in either of these references to make the combination.

The Examiner asserts that the secondary reference of Meyer et al., uses a removable flash memory card in association with currency handling devices. It is believed this seriously mischaracterizes the Meyer et al. reference. The Meyer et al. reference is directed to a fully integrated public telephone system and the flash memory referred to in the Meyer et al. patent is hardwired and integral with the telephone. It is not a removable device and as will be subsequently discussed, all updating of the Meyer et al. device occurs over the public telephone system as discussed according to the security arrangement disclosed in the patent.

The security arrangement clearly uses information associated with the actual telephone device, i.e., the electronic address of the telephone device as opposed to using any information which is inherent to a removable flash memory card. In fact, the Meyer et al. reference does not have a removable flash memory card and the only issue is whether the information that is downloaded to it over the public telephone system is authentic and appropriate for the particular telephone. The evaluation conducted according to the secondary reference is whether this firmware is appropriate for that particular device and is based on information specific to the telephone device.

The Official Action on page 8 states as follows:

"At the time of the invention, it would have been obvious to one of ordinary skill in the art to have used the encryption scheme and flash memory card of Meyer at al. in the bill handling system of Mazur et al.

The suggestion/motivation would have been to use a flash memory card to "promote product firmware security and configuration control"."

Applicant submits this position disregards the teaching of the references.

The secondary reference of Meyer at al. teaches a security arrangement which allows an intelligent telephone with a hardwired flash memory device 5 (see Figure 1) to receive new "firmware" provided to it by the "management system". The telephone is designed to receive and to transmit voice and other communications and the telephone is designed to communicate with the telephone management system from time to time. The Examiner's attention is directed to column 6, lines 28 through 33 where it states:

"The telephone is designed to communicate with the phone management system via a proprietary 1200 baud FSK algorithm. Typically, modem communication is used to poll the installed telephone record, call accounting, and diagnostic information, or for downloading program, rating, or system configuration information."

Column 6, lines 61 to the bottom of the page further describes the primary system component systems of the telephone. It states:

"The primary system memory components are the utility FLASH 5 and data SRAM 6. The phone always boots up from the utility FLASH. The utility FLASH is a downloadable device containing boot code, standard utilities, and voice data. The data SRAM typically contains call rating information, as well as

collected call records. Any of these typical uses may vary by firmware design."

It is apparent from these passages that the FLASH 5 is a downloadable device and is capable of receiving software sent to it over the telephone system from the central office to the particular telephone.

Programming of the FLASH ROM is further described in column 16, lines 37 through 47. Programming of this ROM requires a proprietary interface box and this interface box initiates communication when its switch is turned on but the telephone's microprocessor will work as the master. Basically, the FLASH ROM can receive or has received new firmware for downloading. If this is the case, the device undergoes a security check. Column 17 states:

"To provide for the security required as well as allowing flexibility in implementation, three parameters will be required. The three parameters include configuration code, product code, and revision level."

The purpose of the configuration code is to match the specific group of firmware with the mother board's DS2502. As can be appreciated, the DS2502 is an inherent characteristic of the telephone and is not associated with a removable memory module. A second process is carried out to evaluate information of the DS2502 and an insertable key at JS. Once again, the security check is based on the characteristics of the mother board of the specific telephone.

The product code is subsequently discussed and is a code which is maintained by the mother board's DS2502. If the product

code of the DS2502 does not match with the provided product code, then the telephone will continue to operate in its normal manner.

A careful reading of column 17 and in consideration of Figures 17, 18 and 19 clearly establish that the security check provided in the secondary reference is based on information stored in particular to the particular telephone. Software is downloaded from the central office to the particular telephone. The telephone, then based on information specific to the telephone, is used to evaluate the provided software.

It is clear from the secondary reference that a fully networked system is necessary where the particular device is in full communication with a host office. Furthermore, the security system of this reference requires the particular device to review its own characteristics and conduct its test based on its determined characteristics and information downloaded to it.

The secondary reference is thus in direct contradiction to the present system. It is not practical to have validators which are fully networked. Networking of the validators is not required with the present invention.

It is respectfully submitted that even if the references were combined, they would not arrive at the invention as now claimed. It is critical, according to the secondary reference, to have a fully networked system. There is an integration between the intelligent telephone and the central office. The telephone is provided with a downloadable flash memory which can receive updates from the central office. Any new software which is received by the intelligent telephone is tested based on characteristics specific to the telephone.

If one was to combine this with the primary reference, it is respectfully submitted you would end up with a validator which is networked with the central office. In this way, the security system as taught by the secondary reference could be fully utilized. It is readily apparent that this solution is in contrast to the system presently being claimed.

Even if one was to assume that the flash card of the primary reference should be secure as used in the downloadable memory of the secondary reference, this security would be based on the configuration code, product code and revision level as taught by the secondary reference. Therefore, the security arrangement would require full knowledge of the "configuration code, product code and revision level" of the validator in which the flash memory card was to be used. As indicated in the secondary reference, these are typically unique codes based on the serial numbers provided on the mother boards of the receiving device.

Such as system, which requires full knowledge of the particular validator to be updated, would not be satisfactory. This would require a direct pairing of the removable flash memory device with a particular validator using the specific information of the validator. This does not provide an easy system to update and requires a very efficient and accurate databank of information covering many years.

In contrast, the invention as claimed merely confirms that the software provided to the validator has not been tampered with based on the information provided with the removable memory module and the CPU of the validator then downloads the information after it has decrypted the information. The prior art references do not even suggest such a system. Any further modification of the primary and secondary reference would be in

direct contradiction to the principles set out in these references.

As previously argued, the primary reference has promoted the benefits of the module being capable of being used with many validators and has not appreciated how this arrangement can render the entire system subject to attack or vulnerable. With the present system, all critical information provided in the removable memory module is encrypted and thus, the techniques used by this software to determine the authenticity of banknotes is extremely difficult to determine. This encryption of the software has also encrypted preferably the address of the removable serial module and the validator uses this information as part of its integrity test. If any tampering has occurred to the removable memory module, there will not be a match and the validator will continue to operate in its normal mode.

Method claim 19 has been amended to include the additional step of dependent claim 20. The method of updating the bank validator requires coordination between the removable sensor modules and the removable memory storage arrangement. The claim requires the validator to carry out an evaluation of the updated information prior to installing thereof.

This claim was rejected in view of Mazur et al. in view of Itako et al. and further in view of Meyer et al.

As previously argued, Meyer et al. is truly not directed to the currency validating art. Therefore, the arguments previously submitted regarding the combination of the primary reference and Meyer et al. are reasserted.

It is further argued that there is no teaching to combine the references in this manner. The primary reference has

fixed sensors whereas the secondary reference teaches sensors which are movable within the device. The third reference teaches encryption over a networked system using information specific to the telephone provided by the telephone to a central office which then downloads the information.

The encryption and security technique required of the method claim is not found in the combination and it is again asserted that the only teaching or suggestion for combining the references in this manner is found in the disclosure of the present case. This hindsight analysis and merely using the present disclosure and claims as a road map to selectively identify individual elements to be combined without any suggestion in the references to make this combination is not the appropriate test of obviousness.

The telephone system of the Meyer et al. reference operates on an entirely different basis requiring a complete network system and security being provided by a central office. This is in contrast to a validator which in many cases will be located in a vending machine or device with no ability to communicate to a central source.

The rejection of claims 1 through 20 under the judicially created doctrine of obviousness-type double patenting is traversed. U.S. Patent 6,142,284 does not have a validator adapted to receive a removable memory module. It only teaches removable sensor modules. The secondary reference of Meyer et al. discloses a telephone and a security system for the telephone as it interacts with a central office. Neither reference has a removable memory module nor the cooperation of the validator and the memory module using information inherent to the memory module.

It is therefore submitted this rejection be withdrawn.

Attached on a separate page is a marked up version of the amended claims entitled: VERSION WITH MARKINGS TO SHOW CHANGES.

Reconsideration and allowance of the amended claims is requested.

Respectfully submitted,

Agent on behalf of Applicant
S. Warren Hall
Registration No. 30,350
(416) 368-8313

WH/sdw
Encl.

VERSION WITH MARKINGS TO SHOW CHANGES

Claims 3, 5, 6 and claims 16, 17, 18 and 20 have been cancelled.

Claim 1 has been amended as follows:

1. A banknote validator comprising a banknote processing channel, a series of sensors located along said channel for scanning a banknote as it moves past said sensors, a central processing unit for controlling the operation of said validator and receiving and processing the signals from said sensors, and a removable memory storage arrangement insertable in a receiving location of said validator, said removable memory storage arrangement when received in said receiving location forming an electrical communication path with said central processing unit, said central processing unit including a testing procedure which evaluates the integrity of any received removable memory storage arrangement and said central processing unit downloading information from said received removable storage arrangement for operation thereof upon positive evaluation of the integrity of said removable memory storage arrangement and wherein the removable memory storage arrangement includes an electronic address available to the central processing unit and the electronic address is used as part of said testing procedure and wherein the removable flash memory module contains encrypted algorithms used by the central processing unit to evaluate banknotes for authenticity and the central processing unit includes decryption software for decoding the algorithms and storing the decoded algorithms in said central processing unit.

Claim 19 has been amended as follows:

19. A method of updating the criteria used to evaluate the authenticity of banknotes by a banknote validator having a

banknote processing channel, a series of removable sensor modules located along said channel for scanning a banknote as it moves past said sensor modules, a central processing unit for controlling the operation of said validator and receiving and processing the signals from said sensor modules, and a receiving location for receiving a removable memory storage arrangement and allowing communication between said central processing unit and a received removable memory storage arrangement, said central processing unit including a testing procedure which evaluates the integrity of any received removable memory storage arrangement, said method comprising inserting a removable memory storage arrangement in said receiving arrangement and communicating with said central processing unit, conducting said test procedure using information provided to said central processing unit by said removable memory storage means to confirm the integrity thereof, and in response to confirmation of the integrity of said removable memory storage arrangement downloading information contained in said removable memory storage arrangement to said central processing unit thereby updating the criteria used to evaluate banknotes processed by the validator and including the step of replacing at least one sensor module with a new sensor module and wherein said central processing unit is updated to process the signal of said at least one new sensor module using said downloaded information.